REMARKS

The Applicant appreciates the thorough examination of this application which has been carried out. In this response, Claims 1-5 and 7-16 are amended, Claim 6 is canceled, and new Claims 17-20 are added. Hence, Claims 1-20 are pending in the application.

REJECTIONS/OBJECTIONS NOT BASED ON PRIOR ART

1. DRAWINGS

The drawings were objected to on the grounds that FIG. 1 does not contain the legend "Prior Art" and for failing to comply with 37 CFR 1.84(p)(5). Applicant has carefully reviewed each of the drawings and proposed amendments in a separate Request to For Permission to Amend Drawings addressed to the Official Draftsman.

Approval of the Request is respectfully requested. Applicant proposes to postpone actual correction of the drawings until allowable subject matter is indicated. Applicant believes that each of the objections to the drawings has been addressed.

2. SPECIFICATION

The Office Action objected to the specification as containing grammatical errors and typographical errors. Applicant has thoroughly reviewed the specification and corrected it in this amendment. Applicant believes that all informalities have been addressed.

REJECTIONS BASED ON PRIOR ART

1. CLAIM REJECTIONS - 35 U.S.C. § 102(b)

Claims 1-16 have been rejected under 35 U.S.C. § 102(b) based upon an alleged public use or sale. The rejection is traversed.

Paragraph 10 of the Office Action states that the document entitled "CyberSource IVS" found on the Internet at http://www.cybersource.com/html/solutions/fraud_main.html/#overview is prior art. This is incorrect. Form PTO-1449 issued by the Examiner in this application asserts a publication date of November 4, 1998. Further, the document was first published, in the sense of availability online, in 1998. See Declaration of Thomas A. Arnold, attached ("Arnold Declaration"), at ¶6. Thus, the "CyberSource IVS" document is not prior art to this application. Applicant respectfully requests withdrawal of "CyberSource IVS" as a reference.

The Office Action asserts that "CyberSource IVS" describes the claimed invention and that the claimed invention was originally put into use more than one year prior to the filing of the present application. This is incorrect. The 1996 Press Release, upon which the Office Action relies, does not describe the invention that is disclosed and claimed in the present application. Arnold Declaration, ¶3. Further, the "CyberSource IVS" document does not describe the same software or services as described in the 1996 Press Release.

The software service known as CyberSource IVS 3.0 did not exist in 1996. The first commercial release of a predecessor product that is an embodiment of the subject matter of the present application, "ICS CommerceFLEX, Software Version 2.0," occurred on March 3, 1997. Arnold Declaration, ¶4.

In response to paragraph 13 of the Office Action, at page 14, Applicant has concurrently filed herewith an Information Disclosure Statement and Form PTO-1449 to cite information of the type requested by the Office Action. One of the documents that has been submitted is a copy of a Developer's Guide and Reference for ICS CommerceFLEX, Software Version 2.0, Revision 2.03, April 14, 1997. This document describes an embodiment of the subject matter of this application. Arnold Declaration, ¶5. It is the first published document that describes an embodiment. Id.

Thus, no public use of the subject matter of this application occurred before March 3, 1997, which is less than one year before the filing date of the present application.

The Office Action asserts that "CyberSource IVS" version 3.0 is "fundamentally the same product" as the first released version. This is incorrect. There are numerous differences. For example, ICS CommerceFLEX did not include software or other elements corresponding to an Internet identification verification system as recited in the original claims and as shown in FIG. 4, block 208. Arnold Declaration at ¶7. Further, the consistency check element could not cooperate with the Internet identification verification system, and the databases did not incorporate information from a plurality of merchants. The Internet identification verification system could not be accessed and supplemented by other merchants. Arnold Declaration, ¶7.

While the Assignee of the Applicant placed in commercial use certain software that implemented a limited fraud screening function more than one year before July 28, 1997, that software did not contain all the elements or carry out all the steps that were claimed in the present application as filed.[1] Accordingly, the 1996 Press Release and "CyberSource IVS" do not evidence a public use as asserted by the Office Action and are not proper prior art under 35 U.S.C. § 102(b).

Review of the material filed with the Information Disclosure Statement will show nothing else that evidences a public use or sale of the subject matter of the application. Applicant respectfully requests withdrawal of the 1996 Press Release and "CyberSource IVS" as a reference, and withdrawal of the rejection.

[1] Nothing in this Response states or implies any particular date of invention of the subject matter of this application.

Because "CyberSource IVS" is not a proper reference, the substantive application of "CyberSource IVS" to Claims 1-16, as set forth in the Office Action at pp. 4-8, is believed to be moot and is not addressed herein by the Applicant.

2. REJECTION UNDER § 103(a) (ROSE, SANDBERG-DIMENT, TOM)

Claims 1-9 and 11-15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over ROSE (5757917) in view of SANDBERG-DIMENT (5826245) and TOM (5696907). The rejection is traversed.

The Office Action states:

> "It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine Rose's method for enabling users on the Internet to conduct commercial transactions involving credit card payments with Sandberg-Diment's teachings of verifying the consumer's credit card information based upon a plurality of parameters because it is well known in the art that merchants wishing to protect themselves from credit card fraud ordinarily will perform (or cause to be performed) some type of verification procedure to ensure that a credit card presented for payment by a consumer in a transaction legitimately belongs to him. To verify that a credit card belongs to a consumer in a given transaction, it would be necessary to obtain certain information from him, i.e., a plurality of parameters, and analyze such information to determine whether the credit card does indeed belong to the consumer."

Applicant disagrees. The foregoing statement says no more than what Applicant says about prior art AVS systems of the type shown in FIG. 1 of the specification. The claimed invention, as recited in the amended claims, recites a distinct improvement over AVS systems.

The claimed invention features, among other things, the step of verifying the credit card information based upon transaction values, which may be a plurality of parameters, in combination with information that identifies the consumer, and that may provide an indication whether the credit card transaction is fraudulent. Each value among the plurality of parameters is weighted in the verifying step according to an importance, as determined by the merchant or by transaction processing experience, of that value to the credit card transaction, so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

Applicant has discovered that highly effective fraud detection may be carried out by examining information about a transaction, in combination with information that identifies the consumer. Such external transaction information may include: information indicating whether the proposed, current transaction is consistent with past transactions that the consumer has carried out; information indicating whether the consumer has a history of past fraudulent transactions; information indicating whether the credit card number presented by the consumer is, in fact, authentically associated with the consumer; and information indicating whether the consumer's Internet address is valid. In contrast, information that identifies the consumer includes the consumer's name, address, credit card expiration date, and the consumer's credit card company.

The Office Action states that SANDBERG-DIMENT "teaches verifying the consumer's credit card information based upon a plurality of parameters," but the parameters identified in SANDBERG-DIMENT are only information that identifies a consumer or its card. The method and system disclosed by Applicant goes far beyond this, taking into account a plurality of external factors and other information ("transaction values", "parameters", "checks").

For example, Claim 1, Claim 5, Claim 11, and Claim 15 recite use of transaction values or a plurality of parameters, in combination with information that identifies the consumer, and that may provide an indication whether the credit card transaction is fraudulent. Claim 2, Claim 7, and Claim 12 recite that the parameters specifically include a consistency check, history check, automatic verification system and Internet identification system. These features are not taught, disclosed or suggested by ROSE or SANDBERG-DIMENT, alone or in combination.

Another distinctive feature of Claim 1, Claim 5, Claim 11, and Claim 15, as amended, is that each value among the plurality of parameters is weighted in the verifying step according to an importance, as determined by the merchant, of that value to a determination of fraud in the credit card transaction, so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent. See Specification, pages 2, 4, 5-6. This feature is not taught in the cited art.

The Office Action states:

> "[TOM] teaches weighting the parameters so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent (see column 5, lines 24-57 and column 6, lines 43-46, a neural network is used to provide risk and credit evaluations of newly proposed financial service applications based upon a plurality of parameters which are weighted according to the information contained therein). It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine Rose's teachings and Sandberg-Diment's teachings with Tom's teachings which shows weighting the parameters so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent."

Applicant disagrees. Any "parameters" that may be described in TOM are different from the parameters of the present application. TOM describes weighting nodes of a neural network in which each node corresponds to a value of a variable that describes the consumer. In contrast, the weighting parameters that are disclosed and claimed by Applicant are different classes of tests or checks rather than individual variable values.

In Applicant's disclosure, a "parameter" is a test or check, not a scalar value. This usage may be unconventional, which is permitted, and it is not the same usage as TOM.

Further, risk and credit evaluations of newly proposed financial service applications, as described in TOM, are not the same as fraud detection in a credit card transaction. Risk and credit evaluations involve determining the creditworthiness of an applicant for a loan or other financial service. For example, such evaluations may determine whether the consumer has sufficient available credit to complete a desired transaction. In contrast, fraud detection involves determining whether a consumer offering a credit card number is not actually the cardholder. Applicant has discovered that fraud detection can be carried out effectively based on external transaction information rather than information describing the consumer, including the consumer's amount of available credit. The risk and credit evaluations contemplated by TOM do not involve a loan applicant falsifying his or her identity. In short, TOM addresses a different problem and is improperly combined with ROSE and SANDBERG-DIMENT.

The Office Action further states:

> "In verifying a credit card transaction where a consumer provides certain information as taught by Rose and Sandberg-Diment, one having ordinary skill in the art would have been motivated by Tom to further assign risk factors or weights to each parameter since certain parameters may be more determinant than others towards detecting fraud.

> For example, a parameter containing the cardholder's mother's maiden name would most likely be weighted heavier than a parameter holding the cardholder's last purchase date. Thus, it would be advantageous for a system that detects fraud to place a greater emphasis on the accuracy of crucial data versus possible inaccuracies in less significant values."

Applicant disagrees. No such motivation appears in the references, nor may it be inferred from what is known in the art. TOM only teaches weighting values associated with loan applicant data, whereas Applicant is the first to recognize that a fraud detection system should place weights on different types of checks and tests ("parameters"). Further, Applicant is the first to teach that a fraud detection system should consider information outside the transaction and in combination with personal identifying information associated with the consumer. Any such motivation is apparent only from hindsight. TOM should not be combined with ROSE or SANDBERG-DIMENT.

With respect to Claim 2, the Office Action states:

> "… Tom teaches a method for detecting fraud in a credit card transaction between a consumer and a merchant over the Internet wherein the plurality of parameters includes: a consistency check parameter which is used to determine whether the credit card information is consistent (see figure 7, residence stability, employment stability and miscellaneous); a history check parameter (see figure 7, credit history); an Internet identification system parameter (see figure 7, credit history)."

Applicant disagrees. TOM does not teach a method for detecting fraud in a credit card transaction between a consumer and a merchant over the Internet. TOM teaches a system and method for performing risk and credit analysis of financial service applications, which is fundamentally different from Applicant's system.

TOM does not teach a consistency check parameter which is used to determine whether the credit card information is consistent. TOM teaches analysis of information including residence stability and employment stability. In contrast, Applicant discloses and claims a consistency check parameter, which allows one to determine whether the credit information is consistent, i.e., does the credit information match the user. See Specification at page 5. Residence stability information (whether a consumer has several different past addresses) and employment stability information (whether a consumer has several different past employers) is not the same as testing whether the credit information supplied by the consumer matches the consumer. (The reference in TOM to "miscellaneous" information is impossibly vague and cannot be relied upon to anticipate Applicant's consistency check parameter.)

TOM does not teach a history check parameter. TOM describes considering credit history information. However, the history check taught by Applicant is not credit history information; it is information about prior transactions carried out by the same consumer. TOM does not teach an Internet identification system parameter. That parameter, as taught by Applicant, verifies "whether the Internet address [of the consumer] is consistent with other Internet addresses being used in transactions utilizing this credit card" (Specification, page 5). The Office Action suggests that the "residence stability" information of TOM is an Internet identification system parameter, but this is disingenuous; information about whether a consumer has had multiple residence addresses in a short period of time is not the same as determining whether the same credit card is being used by a consumer claiming several different Internet addresses.

The Office Action further states:

> "TOM fails to teach an automatic verification system parameter. However, official notice is taken that an automatic verification system is an old and well-known type of verification method used in credit card verifications In addition, applicant admits that automatic verification systems are prior art. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine Rose's and Sandberg-Diment's teachings with Tom's teachings …"

Applicant disagrees. Admitting that a particular element is known in the art is not an admission that a combination of that element with others would have been obvious. Carrying out credit card verification, through manual observation or use of an AVS system, is old. But the selection and use of an AVS system, in combination with particular parameters that represent external factors, or information in combination with consumer-identifying information, is not shown anywhere in the art of record. There is no suggestion in the art of record to combine an AVS system with the teachings of the cited art.

The Office Action also states:

> "In addition, a merchant might want to determine whether all the data entered during the transaction by the consumer is consistent, such as the consumer's address and telephone number information (consistency check parameter)."

Applicant is unclear what the Office Action is seeking to convey by this statement or motivation, which is not based on a cited reference. This statement is apparent only after a reading of the present application, and therefore appears to represent impermissible hindsight.

The Office Action then states:

> "One having ordinary skill in the art at the time the invention was made would be motivated further to include an Internet identification parameter because the instant invention is directed towards credit card transactions conducted on the Internet and a merchant wishing to prevent fraud would be inclined to track the Internet address that is being used with the credit card to track where else (other Internet addresses) that specific credit card has been used before. If a merchant determines that the credit card used in a transaction has been used on several different machines possessing different Internet addresses then a greater potential for fraud exists."

Applicant disagrees. Both the motivation and the function described above derive solely from Applicant's specification; no reference is cited and thus there is no teaching of the claimed function. In addition, the Office Action appears to be impermissibly rejecting the claim based on a conclusion of obviousness that is applied to an individual claim step or element. The Office Action must compare and apply the cited art to the claimed combination as a whole, Stratoflex, Inc. v. Aeroquip Corp., 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983); MPEP § 2141.02. The Office Action may not pick and choose elements of the claimed combination, assert that any individual element would have been obvious, and then reject the claimed combination as obvious.

For the reasons given above, it is respectfully submitted that specific elements recited in Claims 1-9, Claims 11-15, and the new claims are not described, shown or suggested by ROSE, SANDBERG-DIMENT, or TOM, alone or in combination. Therefore, Claims 1-9 and 11-15 and the new claims should be allowed over ROSE, SANDBERG-DIMENT, or TOM.

3. CLAIM 3 AND CLAIM 4

With respect to Claim 3 and Claim 4, the Office Action states:

> "... official notice is taken that it is well known in the computer art to use a database that can be accessed by other merchants and a database that can be supplemented by other merchants for the history check parameter."

Applicant disagrees. In the claimed method and system, a merchant and a consumer conduct a transaction, and the merchant relies in part on its database of past transactions to determine whether the current transaction is possibly fraudulent. In addition, the merchant allows other merchants to update the database with information about transactions between the other merchants and the consumer. For example, as stated in the specification, "A key feature of both the history database and the Internet ID database is that they can be accessed and the information therewithin can be supplemented by a variety of other merchants and, therefore, information from those merchants is obtainable thereby." Specification at p. 5. Normally merchant databases are secure to prevent addition or modification of records by unauthorized parties. Applicant is the first to suggest that merchants should cooperate by updating each others' databases with transaction information.

The subject matter of the official notice is not "capable of instant and unquestionable demonstration as being 'well-known' in the art," and Applicant requests the Office to cite a specific reference to substantiate the basis for the official notice. See MPEP § 2144.03.

Also with respect to Claim 3 and Claim 4, the Office Action states:

> "It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Rose, Sandberg-Diment, Tom and the admitted prior art that describe a method for detecting fraud in a credit card transaction between a consumer and a merchant over the Internet with a database that can be accessed by other merchants and a database that can be supplemented by other merchants for the history check parameter since most consumers buy products and services from more than one merchant and thus the only way for one merchant to detect fraud in a credit card transaction would be to have access to

> all of the past transaction history data available from other merchants concerning the specific credit card used in the transaction."

Applicant disagrees. In particular, it is not correct that "the only way for one merchant to detect fraud in a credit card transaction would be to have access to all of the past transaction history data available from other merchants concerning the specific credit card used in the transaction." Conventional practice is for a merchant to secure its own database and prevent third parties, including other merchants, from adding to it. Conventional practice is for the merchant to look only in its own database for records of past transactions with the same consumer.

The argument advanced by the Office Action is not found in the references and cannot be said to be common knowledge or conventional practice. There is no suggestion in the references to combine one with the other. Applicant is the first to suggest that merchants should cooperate by updating each others' databases with transaction information.

For all these reasons, Claim 3 and Claim 4 should be allowed.

CONCLUSION

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of

Allowance is believed next in order, and that action is respectfully requested.

The Examiner may contact the undersigned by telephone if such contact would further the examination of the present application.

Petition for Extension: Applicant hereby petitions, under 37 C.F.R. 1.136, for a one-month extension of time in which to respond to the Office Action, and for such further extensions of time as may be necessary to cause this Response to be timely on the filing date granted to it by the Office.

The Commissioner is authorized to charge the extension fee of $55.00, any other fees due in connection with this response, and to credit any overpayment to Deposit Account No. 50-0385. A duplicate of this paper is filed herewith.

Respectfully submitted,

McDERMOTT, WILL & EMERY

Date: April 21, 1999

Christopher J. Palermo
Reg. No. 42,056

(408) 271-2300
600 13th Street, N.W.
Washington, D.C. 20005

CERTIFICATE OF MAILING

I hereby certify that this correspondencc is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, DC 20231

on 4-21-99 by Kim Arca